

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON

STEPHANIE ESPANOZA, JONATHAN MORALES
and ALEX PYGIN, individually and on behalf of
all others similarly situated,

Plaintiffs,

v.

T-MOBILE USA, INC.,

Defendant.

Case No.

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiffs Stephanie Espanoza, Jonathan Morales and Alex Pygin (“Plaintiffs”) bring this Class Action Complaint against Defendant T-Mobile USA, Inc. (“T-Mobile” or “Defendant”) as individuals and on behalf of all others similarly situated, and allege, upon personal knowledge as to their own actions, their counsel’s investigations, and facts that are a matter of public record, and upon information and belief as to all other matters, as follows:

I. NATURE OF THE ACTION

1. This class action arises out of the recent cyberattack and data breach that was perpetrated against Defendant T-Mobile, a national telecommunications company that provides mobile telephone services to customers throughout the United States (the “Data Breach”). The Data Breach resulted in unauthorized access and exfiltration of highly sensitive and personal information (the “Private Information”).

1 2. As a result of the Data Breach, Plaintiffs and approximately 40 million former or
 2 prospective customers who applied for credit with T-Mobile, 7.8 million current postpaid
 3 customers, and 850,000 active prepaid customers (the “Class Members”)¹ suffered present
 4 injury and damages in the form of identity theft, out-of-pocket expenses and the value of the
 5 time reasonably incurred to remedy or mitigate the effects of the unauthorized access,
 6 exfiltration, and subsequent criminal misuse of their sensitive and highly personal information.

7 3. The Private Information compromised in the Data Breach includes names, phone
 8 numbers, drivers’ licenses, government identification numbers, Social Security numbers, dates
 9 of birth, and T-Mobile account PINs.²

10 4. Plaintiffs bring this class action lawsuit on behalf of those similarly situated to
 11 address Defendant’s inadequate safeguarding of Class Members’ Private Information that it
 12 collected and maintained.

13 5. Defendant maintained the Private Information in a reckless manner. In
 14 particular, the Private Information was maintained on Defendant’s computer system and
 15 network in a condition vulnerable to cyberattacks.

16 6. The mechanism of the cyberattack and potential for improper disclosure of
 17 Plaintiffs’ and Class Members’ Private Information was a known risk to Defendant, and thus
 18 Defendant was on notice that failing to take steps necessary to secure the Private Information
 19 from the risk of a ransomware attack.

20 7. Plaintiffs’ and Class Members’ identities are now at considerable risk because of
 21 Defendant’s negligent conduct since the Private Information that T-Mobile collected and
 22 maintained is now in the hands of data thieves.

23
 24
 25 ¹ See *T-Mobile Shares Additional Information Regarding Ongoing Cyberattack Investigation*, T-Mobile (Aug. 17,
 26 2021), <https://www.t-mobile.com/news/network/additional-information-regarding-2021-cyberattack-investigation> (last visited Aug. 19, 2021).

27 ² *Id.*

1 8. Armed with the Private Information accessed in the Data Breach, data thieves
 2 can commit a variety of crimes, including but not limited to fraudulently applying for
 3 unemployment benefits, opening new financial accounts in Class Members' names, taking out
 4 loans in Class Members' names, using Class Members' information to obtain government
 5 benefits (including unemployment or COVID relief benefits), filing fraudulent tax returns using
 6 Class Members' information, obtaining driver's licenses in Class Members' names but with
 7 another person's photograph and providing false information to police during an arrest.

8 9. Plaintiffs' and Class Members' Private Information was compromised due to
 9 Defendant's negligent and/or careless acts and omissions and its failure to adequately protect
 10 the Private Information of its current, former, and prospective clients.

11 10. As a result of the Data Breach, Plaintiffs and Class Members are exposed to a
 12 heightened present and imminent risk of fraud and identity theft. As a result of Defendant's
 13 actions and inactions, as set forth herein, Plaintiffs and Class Members must now and in the
 14 future closely monitor their financial accounts and information to guard against identity theft,
 15 among other issues.

16 11. Plaintiffs and Class Members have and may in the future incur actual monetary
 17 costs, including but not limited to the cost of purchasing credit monitoring services, credit
 18 freezes, credit reports or other protective measures to deter and detect identity theft.

19 12. Plaintiffs and Class Members have and may in the future expend time spent
 20 mitigating the effects of the Data Breach, including time spent dealing with actual or attempted
 21 fraud and identity theft.

22 13. By their Complaint, Plaintiffs seek to remedy these harms on behalf of
 23 themselves and all similarly situated individuals whose Private Information was accessed during
 24 the Data Breach.

25 14. Accordingly, Plaintiffs bring this action on behalf of all persons whose Private
 26 Information was compromised as a result of Defendant's negligence and failure to: (i)
 27 adequately protect its customer's Private Information, (ii) warn its current, former, and

1 potential customers of their inadequate information security practices, and (iii) effectively
2 monitor their data systems for security vulnerabilities and incidents. Defendant's conduct
3 amounts to negligence and violates federal and state statutes.

4 15. Plaintiffs seek remedies including, but not limited to, compensatory damages,
5 reimbursement of out-of-pocket costs, and injunctive relief including improvements to
6 Defendant's data security systems, future annual audits, and adequate credit monitoring
7 services funded by Defendant.

II. PARTIES

9 16. Plaintiff Stephanie Espanoza is a citizen of California residing in Los Angeles,
10 California.

11 17. Plaintiff Jonathan Morales is a citizen of California residing in Sacramento,
12 California.

18. Plaintiff Alex Pygin is a citizen of California residing in Irvine, California.

14 19. Defendant T-Mobile is a for-profit company incorporated in Delaware with its
15 principal place of business in the State of Washington at 12920 SE 38th St, Bellevue,
16 Washington 98006.

III. JURISDICTION AND VENUE

18 20. This Court has subject matter jurisdiction over this action under 28 U.S.C. §
19 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or
20 value of \$5,000,000, exclusive of interest and costs, there are more than 100 members in the
21 proposed class, and at least one member of the class is a citizen of a state different from
22 Defendant.

23 21. This Court has personal jurisdiction over Defendant because Defendant has its
24 principal place of business is located in the State of Washington.

25 22. Venue is proper in this Court pursuant to 28 U.S.C. § 1331 because a substantial
26 part of the events or omissions giving rise to these claims occurred in, were directed to, and/or

1 emanated from this District. Defendant resides within this judicial district and a substantial part
 2 of the events giving rise to the claims alleged herein occurred within this judicial district.

3 **IV. FACTUAL ALLEGATIONS**

4 **A. Defendant's Business**

5 23. Defendant is a national telecommunications company that provides mobile
 6 communication services, among other products and services, throughout the United States and
 7 around the globe.

8 24. In 2019 alone, T-Mobile claims to have increased its customer base by 7 million
 9 and had revenues totaling \$45 billion.³

10 25. According to Defendant, as of the second quarter of 2021, T-Mobile had 104.8
 11 million customers, making it one of the largest telecommunications providers in the United
 12 States and in the world.⁴

13 26. Upon information and belief, in the ordinary course of doing business,
 14 Defendant collects sensitive Private Information from customers and potential customers such
 15 as:

- 16 • Name;
- 17 • Address;
- 18 • Phone number;
- 19 • Driver's license number;
- 20 • Social Security number;
- 21 • Financial information;
- 22 • Government identification number; and
- 23 • Date of birth.

26 ³ See *Our Story*, T-Mobile, <https://www.t-mobile.com/our-story> (last visited Aug. 19, 2021).

27 ⁴ See *Investor Factbook*, T-Mobile, https://s24.q4cdn.com/400059132/files/doc_financials/2021/q2/NG_TMUS-06_30_2021-EX-99.2.pdf, at p. 6 (last visited Aug. 19, 2021).

1 27. In the course of collecting Private Information from customers and potential
 2 customers, including Plaintiffs and Class Members, Defendant promises to provide
 3 confidentiality and security for customers' and potential customer's Private Information,
 4 including by promulgating and placing privacy policies on its website.

5 28. In the T-Mobile Privacy Notice (hereinafter "Privacy Notice"), which is effective
 6 as of May 5, 2021 and provided on Defendant's website, Defendant states that "[Customers]
 7 trust T-Mobile to connect [customers] to the world every day, and we're working hard to earn a
 8 place in [customers'] heart[s]. A big part of that is maintaining [customer] privacy."⁵

9 29. Further in the Privacy Notice, Defendant promises to protect consumer's Private
 10 Information and that it uses "administrative, technical, contractual, and physical safeguards
 11 designed to protect [customer] data while it is under our control."⁶

12 30. However, Defendant failed to protect and safeguard Plaintiffs' and Class
 13 Members' Private Information. In fact, there is no indication that Defendant followed even its
 14 most basic promises. For example, T-Mobile does not claim that any of the stolen Private
 15 Information was encrypted, including usernames and passwords.

16 **B. The Data Breach**

17 31. On or about August 15, 2021, media reports indicated that T-Mobile was
 18 "investigating a forum post claiming to be selling a mountain of personal data" that had come
 19 from T-Mobile servers that contained personal customer data.⁷

20 32. The reports also claimed that a portion of the stolen T-Mobile customer data,
 21 including "30 million Social Security numbers and drivers licenses," were being sold on the dark
 22 web for approximately \$270,000.⁸

24 ⁵ *T-Mobile Privacy Notice*, T-Mobile, <https://www.t-mobile.com/privacy-center/our-practices/privacy-policy> (last visited Aug. 19, 2021).

25 ⁶ *Id.*

26 ⁷ See Joseph Cox, *T-Mobile Investigating Claims of Massive Customer Data Breach*, Vice (Aug. 15, 2021),
 https://www.vice.com/en/article/akg8wg/tmobile-investigating-customer-data-breach-100-million (last visited Aug. 19, 2021).

27 ⁸ *Id.*

1 33. On August 16, 2021, T-Mobile released a statement that a sophisticated
 2 cyberattack had enabled “unauthorized access to some T-Mobile data” by cyberthieves and
 3 that it had launched an investigation into the Data Breach.⁹

4 34. On August 17, 2021, T-Mobile released a statement saying that “[while] our
 5 investigation is still underway and we continue to learn additional details, we have now been
 6 able to confirm that the data stolen from our systems did include some personal
 7 information.”¹⁰

8 35. On August 19, 2021, T-Mobile posted a “Notice of Data Breach” on its website,
 9 confirming that: “T-Mobile learned that a bad actor illegally accessed personal data. Our
 10 investigation is ongoing, but we have verified that a subset of T-Mobile data had been accessed
 11 by unauthorized individuals and the data stolen from our systems did include some personal
 12 information.”¹¹

13 36. Also on August 19, 2019, T-Mobile began texting the following notice, in part, to
 14 Class Members, including Plaintiffs Espanoza and Morales: “T-Mobile has determined that
 15 unauthorized access to some of your personal data has occurred.”

16 37. In addition, the initial investigation discovered that “7.8 million current T-Mobile
 17 postpaid customer accounts’ information appears to be contained in the stolen files, as well as
 18 just over 40 million records of former or prospective customers who had previously applied for
 19 credit with T-Mobile.”¹²

20 38. T-Mobile also confirmed that the cyberthieves accessed and stole “customers’
 21 first and last names, date of birth, SSN, and driver’s license/ID information for a subset of

22
 23
 24
 25 ⁹ *T-Mobile Cybersecurity Incident Update*, T-Mobile (Aug. 16, 2021), <https://www.t-mobile.com/news/network/cybersecurity-incident-update-august-2021> (last visited Aug. 19, 2021).

26 ¹⁰ *Supra*, note 1.

27 ¹¹ *See Notice of Data Breach: Keeping You Safe from Cybersecurity Threats*, T-Mobile (Aug. 19, 2021), <https://www.t-mobile.com/brand/data-breach-2021> (last visited Aug. 19, 2021).

28 ¹² *Supra*, note 1.

1 current and former postpay customers and prospective T-Mobile customers[,]” as well as
 2 “850,000 active T-Mobile prepaid customer names, phone numbers and account PINs[.]”¹³

3 39. At this time, Defendant has not indicated how long the unauthorized third-party
 4 had unfettered access to sensitive, protected, and confidential customer information stored on
 5 Defendant’s network, such as Plaintiffs’ and Class Members’ Private Information. Had
 6 Defendant taken its data security obligations more seriously, Defendant would have discovered
 7 and stopped the unauthorized intrusion sooner.

8 40. Upon information and belief, the cyberattack was targeted at Defendant due to
 9 its status as a leading telecommunications company that collects and maintains valuable Private
 10 Information, such as Social Security numbers and financial information.

11 41. The targeted cyberattack was expressly designed to gain access to private and
 12 confidential data, including (among other things) the Private Information of current, former,
 13 and prospective customers, like Plaintiffs and the Class Members.

14 42. Because of this targeted cyberattack, data thieves were able to gain access to
 15 Defendant’s servers and subsequently access and exfiltrate the protected Private Information
 16 of Plaintiffs and Class Members.

17 43. By Defendant’s own admission, “we have now been able to confirm that the data
 18 stolen from our systems did include some personal information” which means that Plaintiffs’
 19 and Class Members Private Information was exfiltrated as well, not merely viewed without
 20 authorization.

21 44. The files accessed by this incident contained the following information: names,
 22 dates of birth, phone numbers, drivers’ licenses, government identification numbers, Social
 23 Security numbers, and T-Mobile account PINs

24 45. There is no indication that the Private Information contained in the stolen files
 25 was encrypted.

26

27¹³ *Id.*

1 46. Plaintiffs' Private Information was accessed and stolen in the Data Breach.
 2 Plaintiffs further believe their stolen Private Information was subsequently sold on the Dark
 3 Web.

4 47. Defendant's offer of twenty-four months of complimentary credit monitoring
 5 services is an acknowledgment by T-Mobile that the impacted individuals are subject to a
 6 present and ongoing threat of fraud and identity theft.

7 48. Defendant had obligations created by contract, industry standards, common law,
 8 and representations made to Plaintiffs and Class Members to keep their Private Information
 9 confidential and to protect it from unauthorized access and disclosure.

10 49. Plaintiffs and Class Members provided their Private Information to Defendant
 11 with the reasonable expectation, and mutual understanding, that Defendant would comply
 12 with its obligations to keep such information confidential and secure from unauthorized access.

13 **C. Defendant Was Aware of the Risks of a Data Breach**

14 50. Defendant had obligations created by contract, industry standards, common law,
 15 and representations made to Plaintiffs and Members of the Classes, to keep their Private
 16 Information confidential and to protect it from unauthorized access and disclosure.

17 51. Plaintiffs and Class Members provided their Private Information to Defendant
 18 with the reasonable expectation and mutual understanding that Defendant would comply with
 19 its obligations to keep such information confidential and secure from unauthorized access.

20 52. Defendant's data security obligations were particularly important given the
 21 substantial increase in cyber-attacks and/or data breaches preceding the date of the breach.

22 53. Data breaches have become widespread. For example, the United States saw
 23 1,244 data breaches in 2018 and had 446.5 million exposed records.¹⁴

24
 25
 26
 27 ¹⁴ 98 Must-Know Data Breach Statistics for 2021, Varonis, <https://blogvaronis2.wpengine.com/data-breach-statistics/> (last visited Aug. 19, 2021).

1 54. Defendant clearly understood this reality because a quote, posted on
 2 Defendant's website, by a senior manager of T-Mobiles Cyber Architecture & Controls unit
 3 stated that:

4 At T-Mobile, everyone is challenge[d] to think outside of
 5 conventional approaches to digital security; all know assumptions
 6 are reevaluated. We work on forward-thinking technologies,
 7 including micro-segmentation, machine learning, predictive
 8 analytics, web situational awareness, advance threat mitigation,
 9 active defense, data obfuscation and next-generation endpoint
 10 technologies it.¹⁵

11 55. However, T-Mobile failed to take fully implement data security systems and
 12 protect critical Private Information belonging to consumers.

13 56. Indeed, data breaches, such as the one experienced by Defendant, have become
 14 so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued
 15 a warning to potential targets, so they are aware of, and prepared for, a potential attack.
 16 Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known
 17 and completely foreseeable to the public and to anyone in Defendant's industry, including
 18 Defendant.

19 57. According to the Federal Trade Commission ("FTC"), identity theft wreaks havoc
 20 on consumers' finances, credit history, and reputation and can take time, money, and patience
 21 to resolve.¹⁶ Identity thieves use stolen personal information for a variety of crimes, including
 22 government benefits fraud, phone or utilities fraud, and bank and finance fraud.¹⁷

23

¹⁵ *Digital Security*, T-Mobile, <https://www.t-mobile.com/careers/digital-security> (last visited Aug. 19, 2021).

24 ¹⁶ See *Taking Charge, What to Do If Your Identity is Stolen*, FTC, 3 (Apr. 2013), <https://dss.mo.gov/cd/older-youth-program/files/taking-charge-what-to-do-if-identity-is-stolen.pdf> (last visited Aug. 19, 2021).

25 ¹⁷ *Id.* The FTC defines identity theft as "a fraud committed or attempted using the identifying information of
 26 another person without authority." 16 CFR § 603.2. The FTC describes "identifying information" as "any name or
 27 number that may be used, alone or in conjunction with any other information, to identify a specific person,"
 28 including, among other things, "[n]ame, social security number, date of birth, official State or government issued
 29 driver's license or identification number, alien registration number, government passport number, employer or
 30 taxpayer identification number." See *Taking Charge, What to Do If Your Identity is Stolen*, FTC, 3 (Apr. 2013),
 31 <https://dss.mo.gov/cd/older-youth-program/files/taking-charge-what-to-do-if-identity-is-stolen.pdf> (last visited
 32 Aug. 19, 2021).

1 58. The Private Information of Plaintiffs and Members of the Classes was taken by
 2 hackers to engage in identity theft or and or to sell it to other criminals who will purchase the
 3 Private Information for that purpose. The fraudulent activity resulting from the Data Breach
 4 may not come to light for years.

5 59. Defendant knew, or reasonably should have known, of the importance of
 6 safeguarding the Private Information of Plaintiffs and Members of the Classes, including Social
 7 Security numbers, driver's license, and/or dates of birth, and of the foreseeable consequences
 8 that would occur if Defendant's data security systems were breached, including, specifically,
 9 the significant costs that would be imposed on Plaintiffs and Members of the Classes a result of
 10 a breach.

11 60. Plaintiffs and Members of the Classes now face years of constant surveillance of
 12 their financial and personal records, monitoring, and loss of rights. The Classes are incurring
 13 and will continue to incur such damages in addition to any fraudulent use of their Private
 14 Information.

15 61. The injuries to Plaintiffs and Members of the Classes were directly and
 16 proximately caused by Defendant's failure to implement or maintain adequate data security
 17 measures for the Private Information of Plaintiffs and Members of the Classes.

18 **D. Defendant Failed to Comply with FTC Guidelines**

19 62. The FTC has promulgated numerous guides for businesses which highlight the
 20 importance of implementing reasonable data security practices. According to the FTC, the need
 21 for data security should be factored into all business decision-making.

22 63. In 2016, the FTC updated its publication, Protecting Personal Information: A
 23 Guide for Business, which established cyber-security guidelines for businesses. The guidelines
 24 note that businesses should protect the personal customer information that they keep;
 25 properly dispose of personal information that is no longer needed; encrypt information stored
 26 on computer networks; understand their network's vulnerabilities; and implement policies to
 27

1 correct any security problems. The guidelines also recommend that businesses use an intrusion
 2 detection system to expose a breach as soon as it occurs; monitor all incoming traffic for
 3 activity indicating someone is attempting to hack the system; watch for large amounts of data
 4 being transmitted from the system; and have a response plan ready in the event of a breach.

5 64. The FTC further recommends that companies not maintain Private Information
 6 longer than is needed for authorization of a transaction; limit access to sensitive data; require
 7 complex passwords to be used on networks; use industry-tested methods for security; monitor
 8 for suspicious activity on the network; and verify that third-party service providers have
 9 implemented reasonable security measures.

10 65. The FTC has brought enforcement actions against businesses for failing to
 11 protect consumer data adequately and reasonably, treating the failure to employ reasonable
 12 and appropriate measures to protect against unauthorized access to confidential consumer
 13 data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act
 14 (“FTCA”), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures
 15 businesses must take to meet their data security obligations.

16 66. Defendant failed to properly implement basic data security practices, and their
 17 failure to employ reasonable and appropriate measures to protect against unauthorized access
 18 to consumer Private Information constitutes an unfair act or practice prohibited by Section 5 of
 19 the FTCA, 15 U.S.C. § 45.

20 67. Defendant was at all times fully aware of their obligation to protect the Private
 21 Information of current, former, and prospective customers. Defendant was also aware of the
 22 significant repercussions that would result from their failure to do so.

23 **E. Defendant Failed to Comply with Industry Standards**

24 68. A number of industry and national best practices have been published and
 25 should have been used as a go-to resource and authoritative guide when developing
 26 Defendant’s cybersecurity practices.

1 69. Best cybersecurity practices that are standard in Defendant's industry include
 2 encrypting files; installing appropriate malware detection software; monitoring and limiting the
 3 network ports; protecting web browsers and email management systems; setting up network
 4 systems such as firewalls, switches and routers; monitoring and protection of physical security
 5 systems; protection against any possible communication system; and training staff regarding
 6 critical points.

7 70. Defendant failed to meet the minimum standards of the following cybersecurity
 8 frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-
 9 1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3,
 10 DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's
 11 Critical Security Controls (CIS CSC), which are established standards in reasonable cybersecurity
 12 readiness.

13 71. These foregoing frameworks are existing and applicable industry standards in
 14 Defendant's industry, and Defendant failed to comply with these accepted standards, thereby
 15 opening the door to the Cyber-Attack and causing the Data Breach.

16 **F. Defendant's Breach**

17 72. T-Mobile breached its obligations to Plaintiffs and Class Members and/or was
 18 otherwise negligent and reckless because it failed to properly maintain and safeguard its
 19 computer systems and data. T-Mobile's unlawful conduct includes, but is not limited to, the
 20 following acts and/or omissions:

- 21 a. Failing to maintain an adequate data security system to reduce the risk of
 22 data breaches and cyberattacks;
- 23 b. Failing to adequately protect current, former, and prospective customers'
 24 Private Information;
- 25 c. Failing to properly monitor its own data security systems for existing
 26 intrusions;

- d. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act, and;
- e. Failing to adhere to industry standards for cybersecurity.

73. T-Mobile negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' Private Information.

74. Accordingly, as outlined below, Plaintiffs and Class Members now face an increased risk of fraud and identity theft. In addition, Plaintiffs and the Class Members also lost the benefit of the bargain they made with T-Mobile.

G. The Value of Private Information to Cyber Criminals and Increased Risk of Fraud and Identity Theft to Consumers

75. Businesses that store personal information are likely to be targeted by cyber criminals. Credit card and bank account numbers are tempting targets for hackers. However, information such as dates of birth and Social Security numbers are even more attractive to hackers; they are not easily destroyed and can be easily used to perpetrate identity theft and other types of fraud.

76. The Private Information of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from \$40 to \$200, and bank details have a price range of \$50 to \$200.¹⁸

77. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration (“SSA”) stresses that the loss of an individual’s Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

¹⁸ See *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends, (Oct. 16, 2019), <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs> (last visited Aug. 19, 2021).

1 A dishonest person who has your Social Security number can use it
 2 to get other personal information about you. Identity thieves can
 3 use your number and your good credit to apply for more credit in
 4 your name. Then, they use the credit cards and don't pay the bills,
 5 it damages your credit. You may not find out that someone is using
 6 your number until you're turned down for credit, or you begin to
 7 get calls from unknown creditors demanding payment for items
 8 you never bought. Someone illegally using your Social Security
 9 number and assuming your identity can cause a lot of problems.¹⁹

10 78. What is more, it is no easy task to change or cancel a stolen Social Security
 11 number. An individual cannot obtain a new Social Security number without significant
 12 paperwork and evidence of actual misuse. In other words, preventive action to defend against
 13 the possibility of misuse of a Social Security number is not permitted; an individual must show
 14 evidence of actual, ongoing fraud activity to obtain a new number.

15 79. Even then, a new Social Security number may not be effective. According to Julie
 16 Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link
 17 the new number very quickly to the old number, so all of that old bad information is quickly
 18 inherited into the new Social Security number."²⁰

19 80. Furthermore, as the SSA warns:

20 Keep in mind that a new number probably will not solve all your
 21 problems. This is because other governmental agencies (such as
 22 the IRS and state motor vehicle agencies) and private businesses
 23 (such as banks and credit reporting companies) likely will have
 24 records under your old number. Along with other personal
 25 information, credit reporting companies use the number to identify
 26 your credit record. So using a new number will not guarantee you
 27 a fresh start. This is especially true if your other personal
 information, such as your name and address, remains the same.
 If you receive a new Social Security Number, you should not be able
 to use the old number anymore.

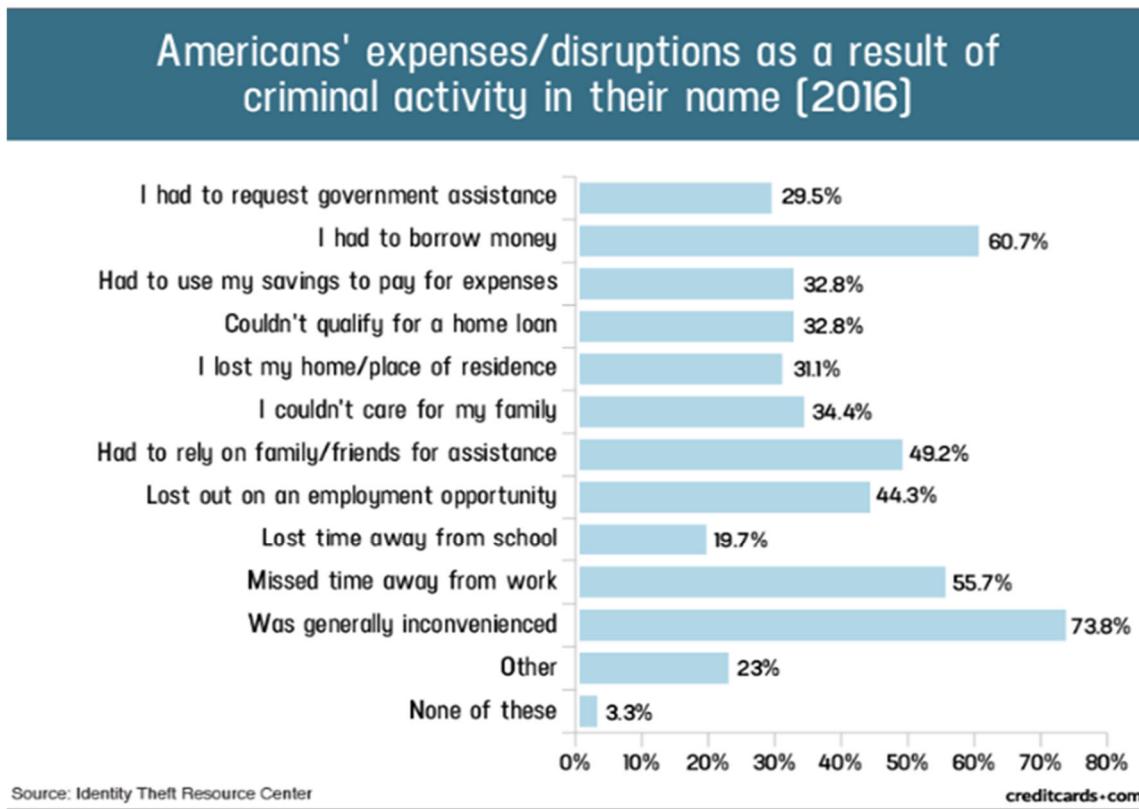
28
 29 25 ¹⁹ *Identity Theft and Your Social Security Number*, Social Security Administration (2018); available at:
 30 <https://www.ssa.gov/pubs/EN-05-10064.pdf> (last visited Aug. 19, 2021).

31 26 ²⁰ Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015),
 32 <http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft> (last visited Aug. 19, 2021).

1 For some victims of identity theft, a new number actually creates
 2 new problems. If the old credit information is not associated with
 3 your new number, the absence of any credit history under the new
 4 number may make more difficult for you to get credit.²¹

5 81. Here, the unauthorized access left the cyber criminals with the tools to perform
 6 the most thorough identity theft—they have obtained all the essential Private Information to
 7 mimic the identity of the user. The personal data of Plaintiffs and Members of the Classes
 8 stolen in the Data Breach constitutes a dream for hackers and a nightmare for Plaintiffs and the
 9 Classes.

10 82. A study by Identity Theft Resource Center shows the multitude of harms caused
 11 by fraudulent use of personal and financial information: ²²



²¹ *Supra*, note 18.

²² See Jason Steele, *Credit Card and ID Theft Statistics*, CreditCards.com (Oct. 23, 2020) <https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php> (last visited Aug. 19, 2021).

1
2 83. Stolen personal data of Plaintiffs and Members of the Classes represents
3 essentially one-stop shopping for identity thieves.

4 84. The FTC has released its updated publication on protecting Private Information
5 for businesses, which includes instructions on protecting Private Information, properly
6 disposing of Private Information, understanding network vulnerabilities, implementing policies
7 to correct security problems, using intrusion detection programs, monitoring data traffic, and
8 having in place a response plan.

9 85. General policy reasons support such an approach. A person whose personal
10 information has been compromised may not see any signs of identity theft for years. According
11 to the United States Government Accountability Office ("GAO") Report to Congressional
12 Requesters:

13 [L]aw enforcement officials told us that in some cases, stolen data
14 may be held for up to a year or more before being used to commit
15 identity theft. Further, once stolen data have been sold or posted
16 on the Web, fraudulent use of that information may continue for
17 years. As a result, studies that attempt to measure the harm
resulting from data breaches cannot necessarily rule out all future
harm.²³

18 86. Companies recognize that Private Information is a valuable asset. Indeed, Private
19 Information is a valuable commodity. A "cyber black-market" exists in which criminals openly
20 post stolen Social Security numbers and other Private Information on a number of Internet
21 websites. The stolen personal data of Plaintiff and members of the Classes has a high value on
22 both legitimate and black markets.

23 87. Identity thieves may commit various types of crimes such as immigration fraud,
24 obtaining a driver's license or identification card in the victim's name but with another's
25

26 ²³ See U.S. Gov. Accounting Office, GAO-07-737, *Personal Information: Data Breaches Are Frequent, but Evidence of*
27 *Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (2007) at 29, available at:
<https://www.gao.gov/new.items/d07737.pdf> (last visited Aug. 19, 2021).

1 picture, and/or using the victim's information to obtain a fraudulent tax refund or fraudulent
 2 unemployment or COVID-19 relief benefits. The United States government and privacy experts
 3 acknowledge that it may take years for identity theft to come to light and be detected.

4 88. As noted above, the disclosure of Social Security numbers in particular poses a
 5 significant risk. Criminals can, for example, use Social Security numbers to create false bank
 6 accounts or file fraudulent tax returns. Defendant's current, former, and prospective customers
 7 whose Social Security numbers have been compromised now face a present and imminent risk
 8 of identity theft and other problems associated with the disclosure of their Social Security
 9 number and will need to monitor their credit and tax filings for an indefinite duration.

10 89. Based on the foregoing, the information compromised in the Data Breach is
 11 significantly more valuable than the loss of, for example, credit card information in a retailer
 12 data breach, because, there, victims can cancel or close credit and debit card accounts. The
 13 information compromised in this Data Breach is impossible to "close" and difficult, if not
 14 impossible, to change — Social Security number, driver's license number or government-issued
 15 identification number, name, and date of birth.

16 90. This data demands a much higher price on the black market. Martin Walter,
 17 senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information,
 18 personally identifiable information and Social Security numbers are worth more than 10x on
 19 the black market."²⁴

20 91. Among other forms of fraud, identity thieves may obtain driver's licenses,
 21 government benefits, medical services, and housing or even give false information to police.

22 92. According to a recent article in the New York Times, cyber thieves are using
 23 illegally obtained driver's to submit and fraudulently obtain unemployment benefits.²⁵ An
 24

25 ²⁴ Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), <https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html> (last visited Aug. 19, 2021).

26 ²⁵ *How Identity Thieves Took My Wife for a Ride*, New York Times, (April 27, 2021)
 27 <https://www.nytimes.com/2021/04/27/your-money/identity-theft-auto-insurance.html> (last visited Aug. 19, 2021)

1 individual may not know that his or her driver's license was used to file for unemployment
 2 benefits until law enforcement notifies the individual's employer of the suspected fraud, or
 3 until the individual attempts to lawfully apply for unemployment and is denied benefits (due to
 4 the prior, fraudulent application and award of benefits).

5 **H. The Plaintiffs' Experiences**

6 **1. Plaintiff Stephanie M. Espanoza**

7 93. Plaintiff Stephanie Espanoza opened her cellular telephone postpaid customer
 8 account with Defendant in or about June 2006 and was required to provide, among other
 9 things, her full name, date of birth and Social Security number.

10 94. On or about August 16, 2021, Plaintiff Espanoza, and the public, was first notified
 11 of the Data Breach by T-Mobile and that cybercriminals had illegally accessed and stole
 12 confidential customer data from millions of T-Mobile customer accounts. In addition, Plaintiff
 13 Espanoza received the August 19, 2021 text message from T-Mobile notifying her that her
 14 Private Information was among the confidential data that cybercriminals illegally accessed and
 15 stole from Defendant's servers.

16 95. As a direct and proximate result of the breach, Plaintiff Espanoza has made
 17 reasonable efforts to mitigate the impact of the breach, including but not limited to: purchasing
 18 credit protection, researching the internet concerning this Data Breach; discussing the breach
 19 with her family; reviewing credit reports and financial account statements for any indications of
 20 actual or attempted identity theft or fraud; and researching credit monitoring and identity theft
 21 protection services offered by Defendant. This is valuable time Plaintiff Espinoza otherwise
 22 could have and would have spent on other activities, including but not limited to taking care of
 23 her 10-month old daughter, work and/or recreation.

24 96. Plaintiff Espinoza is very concerned about identity theft, her banking account and
 25 fraud, as well as the consequences of such identity theft and fraud resulting from the Data
 26 Breach.

1 97. Plaintiff Espinoza suffered actual injury from having Private Information
 2 compromised as a result of the Data Breach including, but not limited to (a) damage to and
 3 diminution in the value of his Private Information, a form of property that Defendant obtained
 4 from Plaintiff; (b) violation of Plaintiffs' privacy rights; and (c) present and increased risk arising
 5 from the identity theft and fraud.

6 98. Plaintiff Espinoza has and will spend a significant amount of time responding to
 7 the impacts of the Data Breach. The time spent dealing with the fallout from the Data Breach is
 8 time Plaintiff otherwise would have spent on other activities, such as caring for her newborn,
 9 work and/or recreation.

10 99. As a result of the Data Breach, Plaintiff Espinoza anticipates spending
 11 considerable time and money on an ongoing basis to try to mitigate and address harms caused
 12 by the Data Breach. As a result of the Data Breach, Plaintiff is and will continue to be at
 13 increased risk of identity theft and fraud for years to come.

14 2. **Plaintiff Jonathan Morales**

15 100. Plaintiff Jonathan Morales is a T-Mobile cellular customer and was required to
 16 provide to Defendant, among other things, his full name and Social Security number.

17 101. On or about August 17, 2021, Plaintiff Morales, and the public, was first notified
 18 of the Data Breach by T-Mobile and that cybercriminals had illegally accessed and stole
 19 confidential customer data from millions of T-Mobile customer accounts. In addition, Plaintiff
 20 Morales received the August 19, 2021 text message from T-Mobile notifying him that his
 21 Private Information was among the confidential data that cybercriminals illegally accessed and
 22 stole from Defendant's servers.

23 102. As a direct and proximate result of the breach, Plaintiff Morales has made
 24 reasonable efforts to mitigate the impact of the breach, including but not limited to:
 25 researching the Data Breach; reviewing credit reports and financial account statements for any
 26 indications of actual or attempted identity theft or fraud; and researching credit monitoring and
 27

1 identity theft protection services offered by Defendant. This is valuable time Plaintiff Morales
 2 otherwise would have spent on other activities, including but not limited to work and/or
 3 recreation.

4 103. Plaintiff Morales is very concerned about identity theft and fraud, as well as the
 5 consequences of such identity theft and fraud resulting from the Data Breach.

6 104. Plaintiff Morales suffered actual injury from having Private Information
 7 compromised as a result of the Data Breach including, but not limited to (a) damage to and
 8 diminution in the value of his Private Information, a form of property that Defendant obtained
 9 from Plaintiff; (b) violation of Plaintiffs' privacy rights; and (c) present and increased risk arising
 10 from the identity theft and fraud.

11 105. Moreover, subsequent to the Data Breach, Plaintiff Morales also experienced a
 12 significant increase in the amount of suspicious, unsolicited phishing spam. Plaintiff Morales
 13 receives a substantial amount of spam, all of which appear to be placed with the intent to
 14 obtain personal information to commit identity theft by way of a social engineering attack.

15 106. Plaintiff Morales has and will spend a significant amount of time responding to
 16 the impacts of the Data Breach. The time spent dealing with the fallout from the Data Breach is
 17 time Plaintiff otherwise would have spent on other activities, such as work and/or recreation.

18 107. As a result of the Data Breach, Plaintiff Morales anticipates spending
 19 considerable time and money on an ongoing basis to try to mitigate and address harms caused
 20 by the Data Breach. As a result of the Data Breach, Plaintiff is and will continue to be at
 21 increased risk of identity theft and fraud for years to come.

22 3. **Plaintiff Alex Pygin**

23 108. Plaintiff Alex Pygin opened his cellular telephone postpaid customer account
 24 with Defendant in or about August 2019 and was required to provide, among other things, his
 25 full name and Social Security number.

1 109. On or about August 17, 2021, Plaintiff Pygin, and the public, was first notified of
 2 the Data Breach by T-Mobile and that cybercriminals had illegally accessed and stole
 3 confidential customer data from millions of T-Mobile customer accounts.²⁶

4 110. As a direct and proximate result of the breach, Plaintiff Pygin has made
 5 reasonable efforts to mitigate the impact of the breach, including but not limited to:
 6 researching the Data Breach; reviewing credit reports and financial account statements for any
 7 indications of actual or attempted identity theft or fraud; and researching credit monitoring and
 8 identity theft protection services offered by Defendant. This is valuable time Plaintiff Pygin
 9 otherwise would have spent on other activities, including but not limited to work and/or
 10 recreation.

11 111. Plaintiff Pygin is very concerned about identity theft and fraud, as well as the
 12 consequences of such identity theft and fraud resulting from the Data Breach.

13 112. Plaintiff Pygin suffered actual injury from having Private Information
 14 compromised as a result of the Data Breach including, but not limited to (a) damage to and
 15 diminution in the value of his Private Information, a form of property that Defendant obtained
 16 from Plaintiff; (b) violation of Plaintiffs' privacy rights; and (c) present and increased risk arising
 17 from the identity theft and fraud.

18 113. Plaintiff Pygin has and will spend a significant amount of time responding to the
 19 impacts of the Data Breach. The time spent dealing with the fallout from the Data Breach is
 20 time Plaintiff otherwise would have spent on other activities, such as work and/or recreation.

21 114. As a result of the Data Breach, Plaintiff Pygin anticipates spending considerable
 22 time and money on an ongoing basis to try to mitigate and address harms caused by the Data
 23 Breach. As a result of the Data Breach, Plaintiff is and will continue to be at increased risk of
 24 identity theft and fraud for years to come.

25
 26
 27 ²⁶ *Supra*, note 1.

1 **I. Plaintiffs' and Class Members' Damages**

2 115. To date, Defendant has done absolutely nothing to provide Plaintiffs and Class
 3 Members with relief for the damages they have suffered because of the Data Breach, including,
 4 but not limited to, the costs and loss of time they incurred because of the Data Breach.

5 116. Defendant has only offered inadequate identity monitoring services. Defendant
 6 places the burden squarely on Plaintiffs and Class Members by requiring them to expend time
 7 signing up for that service, as opposed to automatically enrolling all victims of this cybercrime.
 8 In addition, Defendant only offers these services for two years, even though experts agree that
 9 the effects of such a data breach can often be felt by victims for around seven years.

10 117. Plaintiffs' and Class Members' Private Information were compromised as a direct
 11 and proximate result of the Data Breach.

12 118. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class
 13 Members are in imminent, immediate, and continuing increased risk of harm from fraud and
 14 identity theft.

15 119. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class
 16 Members have been forced to expend time dealing with the effects of the Data Breach.

17 120. Plaintiffs and Class Members face a present and substantial risk of out-of-pocket
 18 fraud losses such as loans opened in their names, government benefits fraud, tax return fraud,
 19 utility bills opened in their names, credit card fraud, and similar identity theft.

20 121. Plaintiffs and Class Members face a present and substantial risk of being targeted
 21 for future phishing, data intrusion, and other illegal schemes based on their Private Information
 22 as potential fraudsters could use that information to target such schemes more effectively to
 23 Plaintiffs and Class Members.

24 122. Plaintiffs and Class Members have and may continue to incur out-of-pocket costs
 25 for protective measures such as credit monitoring fees, credit report fees, credit freeze fees,
 26 and similar costs directly or indirectly related to the Data Breach.

1 123. Plaintiffs and Class Members also suffered a loss of value of their Private
 2 Information when it was acquired by cyber thieves in the Data Breach. Numerous courts have
 3 recognized the propriety of loss of value damages in related cases.

4 124. Plaintiffs and Class Members have spent and will continue to spend significant
 5 amounts of time to monitor their financial accounts for misuse. Indeed, Defendant's own
 6 Notice of Data Breach page posted on its website states that the stolen data is in "harm's way"
 7 and encourages Plaintiffs and Class Members to "take proactive steps regularly to protect your
 8 data and identity[.]" ²⁷

9 125. Plaintiffs and Class Members have suffered or will suffer actual injury as a direct
 10 result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-
 11 pocket expenses and the value of their time reasonably incurred to remedy or mitigate the
 12 effects of the Data Breach relating to:

- 13 a. Finding fraudulent charges, loans, and/or government benefit claims;
- 14 b. Purchasing credit monitoring and identity theft prevention;
- 15 c. Placing "freezes" and "alerts" with credit reporting agencies;
- 16 d. Spending time on the phone with or at a financial institution or
 government agency to dispute fraudulent charges and/or claims;
- 17 e. Contacting financial institutions and closing or modifying financial
 accounts;
- 18 f. Closely reviewing and monitoring Social Security numbers, bank
 accounts, and credit reports for unauthorized activity for years to come.

22 126. Moreover, Plaintiffs and Class Members have an interest in ensuring that their
 23 Private Information, which is believed to remain in the possession of Defendant, is protected
 24 from further breaches by the implementation of security measures and safeguards, including
 25 but not limited to, making sure that the storage of data or documents containing personal and

27 ²⁷ *Notice of Data Breach: Keeping You Safe from Cybersecurity Threats*, T-Mobile (Aug. 19, 2021), <https://www.t-mobile.com/brand/data-breach-2021> (last visited Aug. 19, 2021).

1 financial information is not accessible online, that access to such data is password-protected,
2 and that such data is properly encrypted.

3 127. As a direct and proximate result of Defendant's actions and inactions, Plaintiffs
4 and Class Members have suffered a loss of privacy and are at an imminent and increased risk of
5 future harm.

6 128. To date, Defendant has done absolutely nothing to provide Plaintiffs and Class
7 members with relief for the damages they have suffered because of the Data Breach, including,
8 but not limited to, the costs and loss of time they incurred because of the Data Breach.

9 129. Defendant has only offered inadequate identity monitoring services, and it is
10 unclear whether that credit monitoring was only offered to certain affected individuals (based
11 upon the type of data stolen), or to all persons whose data was compromised in the Data
12 Breach. What is more, Defendant places the burden squarely on Plaintiffs and Class members
13 by requiring them to expend time signing up for that service, as opposed to automatically
14 enrolling all victims of this cybercrime.

V. CLASS ALLEGATIONS

16 130. Plaintiffs bring this nationwide class action pursuant to rules 23(b)(2), 23(b)(3),
17 and 23(c)(4) of the Federal Rules of Civil Procedure, individually and on behalf of all members of
18 the following class:

19 All current, former, and prospective T-Mobile customers residing in
20 the United States whose Private Information was compromised in
21 the Data Breach announced by Defendant on or about August 16,
2021 (the “Nationwide Class”).

22 131. The California Subclass is defined as follows:

23 All current, former, and prospective T-Mobile customers residing
24 in California whose Private Information was compromised in the
25 Data Breach announced by Defendant on or about August 16,
2021 (the “California Subclass”).

1 132. The California Subclass is referred to herein as the "Statewide Subclass" and
 2 together with the Nationwide Class, are collectively referred to herein as the "Classes."

3 133. Excluded from the Classes are all individuals who make a timely election to be
 4 excluded from this proceeding using the correct protocol for opting out, and all judges assigned
 5 to hear any aspect of this litigation and their immediate family members.

6 134. Plaintiffs reserve the right to modify or amend the definitions of the proposed
 7 Classes before the Court determines whether certification is appropriate.

8 135. **Numerosity:** The Classes are so numerous that joinder of all members is
 9 impracticable. Defendant has identified millions of current, former, and prospective customers
 10 whose Private Information may have been improperly accessed in the Data Breach, and the
 11 Classes are apparently identifiable within Defendant's records.

12 136. **Commonality:** Questions of law and fact common to the Classes exist and
 13 predominate over any questions affecting only individual members of the Classes. These
 14 include:

- 15 a. When Defendant actually learned of the Data Breach and whether their
 16 response was adequate;
- 17 b. Whether Defendant owed a duty to the Classes to exercise due care in
 18 collecting, storing, safeguarding and/or obtaining their Private
 19 Information;
- 20 c. Whether Defendant breached that duty;
- 21 d. Whether Defendant implemented and maintained reasonable security
 22 procedures and practices appropriate to the nature of storing the Private
 23 Information of Plaintiffs and Members of the Classes;
- 24 e. Whether Defendant acted negligently in connection with the monitoring
 25 and/or protection of Private Information belonging to Plaintiffs and
 26 Members of the Classes;

- 1 f. Whether Defendant knew or should have known that it did not employ
- 2 reasonable measures to keep the Private Information of Plaintiffs and
- 3 Members of the Classes secure and to prevent loss or misuse of that
- 4 Private Information;
- 5 g. Whether Defendant adequately addressed and fixed the vulnerabilities
- 6 which permitted the Data Breach to occur;
- 7 h. Whether Defendant caused Plaintiffs' and Members of the Classes
- 8 damage;
- 9 i. Whether Defendant violated the law by failing to promptly notify
- 10 Plaintiffs and Members of the Classes that their Private Information had
- 11 been compromised;
- 12 j. Whether Defendant violated the consumer protection statutes invoked
- 13 below; and
- 14 k. Whether Plaintiffs and the other Members of the Classes are entitled to
- 15 credit monitoring and other monetary relief;

16 137. **Typicality:** Plaintiffs' claims are typical of those of the other Members of the
17 Classes because all had their Private Information compromised as a result of the Data Breach
18 due to Defendant's misfeasance.

19 138. **Adequacy:** Plaintiffs will fairly and adequately represent and protect the
20 interests of the members of the Classes. Plaintiffs' Counsel are competent and experienced in
21 litigating privacy-related class actions.

22 139. **Superiority and Manageability:** Under rule 23(b)(3) of the Federal Rules of Civil
23 Procedure, a class action is superior to other available methods for the fair and efficient
24 adjudication of this controversy since joinder of all the members of the Classes is impracticable.
25 Individual damages for any individual member of the Classes are likely to be insufficient to
26 justify the cost of individual litigation, so that in the absence of class treatment, Defendant's
27 misconduct would go unpunished. Furthermore, the adjudication of this controversy through a

1 class action will avoid the possibility of inconsistent and potentially conflicting adjudication of
 2 the asserted claims. There will be no difficulty in the management of this action as a class
 3 action.

4 140. Class certification is also appropriate under Rule 23(a) and (b)(2) because
 5 Defendant acted or refused to act on grounds generally applicable to the Classes, so that final
 6 injunctive relief or corresponding declaratory relief is appropriate as to the Nationwide Class as
 7 a whole and as to the Subclass as a whole.

8 141. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification
 9 because such claims present only particular, common issues, the resolution of which would
 10 advance the disposition of this matter and the parties' interests therein. Such particular issues
 11 include, but are not limited to:

- 12 a. Whether Defendant owed a legal duty to Plaintiffs and Members of the
 13 Classes to exercise due care in collecting, storing, using, and safeguarding
 14 their Private Information;
- 15 b. Whether Defendant breached a legal duty to Plaintiffs and the Members
 16 of the Classes to exercise due care in collecting, storing, using, and
 17 safeguarding their Private Information;
- 18 c. Whether Defendant failed to comply with its own policies and applicable
 19 laws, regulations, and industry standards relating to data security;
- 20 d. Whether Defendant failed to implement and maintain reasonable
 21 security procedures and practices appropriate to the nature and scope of
 22 the information compromised in the Data Breach; and
- 23 e. Whether members of the Classes are entitled to actual damages, credit
 24 monitoring or other injunctive relief, and/or punitive damages as a result
 25 of Defendant's wrongful conduct.

VI. FIRST CLAIM FOR RELIEF

Negligence (On Behalf of Plaintiffs, the Nationwide Class, and the Statewide Subclass)

142. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 141.

143. Defendant owed a common law duty to Plaintiffs and Members of the Classes to exercise reasonable care in obtaining, using, and protecting their Private Information from unauthorized third parties.

144. The legal duties owed by Defendant to Plaintiffs and Members of the Classes include, but are not limited to the following:

- a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information of Plaintiffs and Members of the Classes in its possession;
- b. To protect Private Information of Plaintiffs and Members of the Classes in its possession using reasonable and adequate security procedures that are compliant with industry-standard practices; and
- c. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches, including promptly notifying Plaintiffs and Members of the Classes of the Data Breach.

145. Defendant’s duty to use reasonable data security measures also arose under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45(a) (the “FTC Act”), which prohibits “unfair . . . practices in or affecting commerce,” including, as interested and enforced by the Federal Trade Commission, the unfair practices by companies such as Defendant of failing to use reasonable measures to protect Private Information.

146. Various FTC publications and data security breach orders further form the basis of Defendant's duty. Plaintiffs and Members of the Classes are consumers under the FTC Act. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect Private Information and by not complying with industry standards.

147. Defendant breached its duties to Plaintiffs and Members of the Classes.

Defendant knew or should have known the risks of collecting and storing Private Information and the importance of maintaining secure systems, especially in light of the fact that data breaches have been surging in the past 5 years.

148. Defendant knew or should have known that its security practices did not adequately safeguard the Private Information belonging to the Plaintiffs and Members of the Classes.

149. Through Defendant's acts and omissions described in this Complaint, including Defendant's failure to provide adequate security and its failure to protect the Private Information of Plaintiffs and Members of the Classes from being foreseeably captured, accessed, exfiltrated, stolen, disclosed, and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure the Private Information of Plaintiffs and Members of the Classes during the period it was within Defendant's possession and control.

150. Defendant breached the duties it owed to Plaintiffs and Members of the Classes in several ways, including:

- a. Failing to implement adequate security systems, protocols, and practices sufficient to protect current, former, and prospective customers' Private Information, including Plaintiffs and Members of the Classes, and thereby creating a foreseeable risk of harm;

b. Failing to comply with the minimum industry data security standards prior to the Data Breach;

- c. Failing to act despite knowing or having reason to know that its systems were vulnerable to attack; and

151 Due to Defendant's conduct, Plaintiffs and Members of the Classes are entitled

to credit monitoring. Credit monitoring is reasonable here. The Private Information taken can be used for identity theft and other types of financial fraud against Plaintiffs and Members of the Classes.

152. Some experts recommend that data breach victims obtain credit monitoring services for at least ten years following a data breach. Annual subscriptions for credit monitoring plans range from approximately \$219 to \$358 per year.²⁸

153. As a result of Defendant's negligence, Plaintiffs and Members of the Classes suffered injuries that may include: (i) the lost or diminished value of Private Information; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including, but not limited to, time spent deleting phishing scams and reviewing and monitoring sensitive accounts; (iv) the present and continued risk to their Private Information, which may remain for sale on the dark web and is in Defendant's possession and subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in their continued possession; (v) future costs in terms of time, effort, and money that will be expended to prevent, monitor, detect, contest, and repair the impact of the Data Breach for the remainder of the lives of Plaintiffs and Members of the Classes, including ongoing credit monitoring.

154. These injuries were reasonably foreseeable given the history of security breaches of this nature. The injury and harm that Plaintiff and the members of the Classes suffered was the direct and proximate result of Defendant's negligent conduct.

VII. SECOND CLAIM FOR RELIEF

Negligence *Per Se* (On Behalf of Plaintiffs, the Nationwide Class, and the Statewide Subclass)

155. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 141.

²⁸ In the recent Equifax data breach, for example, Equifax agreed to free monitoring of victims' credit reports at all three major credit bureaus for four years, plus \$1 million of identity theft insurance. For an additional six years, victims can opt for free monitoring by one credit bureau, Equifax. In addition, if a victim's child was a minor in May 2017, he or she is eligible for a total of 18 years of free credit monitoring under the same terms as for adults.

1 156. Section 5 of the FTC Act prohibits “unfair . . . practices in or affecting commerce,”
 2 including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such
 3 as Defendant’s, of failing to use reasonable measures to protect Private Information. The FTC
 4 publications and orders described above also form part of the basis of Defendant’s duty in this
 5 regard.

6 157. Defendant violated Section 5 of the FTC Act by failing to use reasonable
 7 measures to protect Private Information and not complying with applicable industry standards.
 8 Defendant’s conduct was particularly unreasonable given the nature and amount of Private
 9 Information it obtained and stored, and the foreseeable consequences of the Data Breach for
 10 companies of Defendant’s magnitude, including, specifically, the immense damages that would
 11 result to Plaintiffs and Members of the Classes due to the valuable nature of the Private
 12 Information at issue in this case—including Social Security numbers.

13 158. Defendant’s violations of Section 5 of the FTC Act constitute negligence per se.

14 159. Plaintiffs and Members of the Classes are within the class of persons that the FTC
 15 Act was intended to protect.

16 160. The harm that occurred as a result of the Data Breach is the type of harm the
 17 FTC Act was intended to guard against. The FTC has pursued enforcement actions against
 18 businesses, which, as a result of its failure to employ reasonable data security measures and
 19 avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and
 20 Members of the Classes.

21 161. As a direct and proximate result of Defendant’s negligence per se, Plaintiffs and
 22 Members Classes have suffered and will suffer injury, including but not limited to: (i) actual
 23 identity theft; (ii) the loss of the opportunity how their Private Information is used; (iii) the
 24 compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses
 25 associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or
 26 unauthorized use of their Private Information; (v) lost opportunity costs associated with effort
 27 expended and the loss of productivity addressing and attempting to mitigate the actual and

1 future consequences of the Data Breach, including but not limited to efforts spent researching
2 how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs
3 associated with placing freezes on credit reports; (vii) the present and continued risk to their
4 Private Information, which remains in Defendant's possession and is subject to further
5 unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate
6 measures to protect the Private Information of its current, former, and prospective customers
7 in its continued possession; and (viii) future costs in terms of time, effort, and money that will
8 be expended to prevent, detect, contest, and repair the impact of the Private Information
9 compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and
10 Members of the Classes.

11 162. Additionally, as a direct and proximate result of Defendant's negligence *per se*,
12 Plaintiffs and Members of the Classes have suffered and will suffer the continued risks of
13 exposure of their Private Information, which remains in Defendant's possession and is subject
14 to further unauthorized disclosures so long as Defendant fails to undertake appropriate and
15 adequate measures to protect the Private Information in their continued possession.

VIII. THIRD CLAIM FOR RELIEF

Breach of Implied Contract

(On Behalf of Plaintiffs, the Nationwide Class, and the Statewide Subclass)

19 163. Plaintiffs re-allege and incorporate by reference Paragraphs 1 through 141 above
20 as if fully set forth herein.

164. Defendant provided Plaintiffs and Class Members with an implied contract to
protect and keep confidential Defendant's current, former, and prospective customers' private,
nonpublic personal and financial information when they gathered the information from each of
their current, former, and prospective customers.

25 165. Plaintiffs and Class Members would not have provided their personal and
26 financial information to Defendant, but for Defendant's implied promises to safeguard and

1 protect Defendant's current, former, and prospective customers private personal and financial
2 information.

3 166. Plaintiffs and Class Members performed their obligations under the implied
4 contract when they provided their private personal and financial information in exchange for
5 telecommunication services provided by Defendant.

6 167. Defendant breached the implied contracts with Plaintiffs and Class Members by
7 failing to protect and keep private the nonpublic personal and financial information provided to
8 them about Plaintiffs and Class Members.

9 168. As a direct and proximate result of Defendant's breach of their implied contracts,
10 Plaintiffs and Class Members have been harmed and have suffered, and will continue to suffer,
11 damages and injuries.

12 **IX. FOURTH CLAIM FOR RELIEF**

13 **Violations of California's Consumer Legal Remedies Act Cal. Civ. Code § 1750, *et seq.***

14 **(On Behalf of Plaintiffs and the Statewide Subclass)**

15 169. Plaintiffs re-allege and incorporate by reference herein all of the allegations
16 contained in paragraphs 1 through 141.

17 170. Plaintiffs bring this claim individually and on behalf of the Members of the
18 Statewide Subclass.

19 171. Defendant's conduct constitutes violations under California's Legal Remedies
20 Act, Cal. Civ. Code § 1750, *et seq.* (the "CLRA").

21 172. Defendant's conduct falls within the meaning of this statute because they caused
22 transactions resulting in the sale or lease of goods or services to consumers – namely, the sale
23 of cellular products and services to consumers. Such as Plaintiffs and Class Members. The sale
24 of these cellular services is considered services within the meaning of the statute under Civil
25 Code § 1761(b).

26

27

173. Plaintiffs and Members of the Statewide Subclass are consumers pursuant to this statute.

174. Defendant violated the Consumer Legal Remedies Act by way of Civil Code § 1770(a)(5). In particular, Defendant represented (and continues to represent) that their services have benefits and characteristics which they do not have – mainly that Defendant has adequate data security practices to ensure that consumers' Private Information is safe and secure from unauthorized disclosure.

175. Defendant is aware that this misrepresentation, which is a significant factor for its commercial success, is false and misleading.

176. Plaintiffs and Members of the Statewide Class seek injunctive or other equitable relief to ensure that Defendant hereinafter adequately safeguards Private Information by implementing reasonable security procedures and practices. This relief is important because Defendant still holds Private Information related to Plaintiffs and Members of the Statewide Class. Plaintiffs and Members of the California Class have an interest in ensuring that their Private Information is reasonably protected.

177. Pursuant to Cal. Civ. Code § 1782, on August 20, 2011, Plaintiffs will mail Defendant notice in writing, via U.S. certified mail, of the particular violations of Cal. Civ. Code § 1770 of the CLRA and demand that they rectify the actions described above by providing complete monetary relief, agreeing to be bound by Defendant's legal obligations and to give notice to all affected customers of their intent to do so. If Defendant fails to take the actions demanded to rectify their violations of the CLRA, Plaintiffs will seek statutory damages and attorneys' fees as allowed by the CLRA.

X. FIFTH CLAIM FOR RELIEF

Violation of the Washington State Consumer Protection Act (RCW 19.86.010 *et seq.*)

(On Behalf of Plaintiffs and the Nationwide Class)

1 178. Plaintiffs re-allege and incorporate by reference Paragraphs 1 through 141 above
2 as if fully set forth herein.

3 179. The Washington State Consumer Protection Act, RCW 19.86.020 (the “CPA”)
4 prohibits any “unfair or deceptive acts or practices” in the conduct of any trade or commerce as
5 those terms are described by the CPA and relevant case law.

6 180. Defendant is a “person” as described in RWC 19.86.010(1).

7 181. Defendant engages in “trade” and “commerce” as described in RWC
8 19.86.010(2) in that they engage in selling telecommunication products and services, that
9 directly and indirectly affect the people of the State of Washington.

10 182. By virtue of the above-described wrongful actions, inaction, omissions, and want
11 of ordinary care that directly and proximately caused the Data Breach, Defendant engaged in
12 unlawful, unfair and fraudulent practices within the meaning, and in violation of, the CPA, in
13 that Defendant’s practices were injurious to the public interest because they injured other
14 persons, had the capacity to injure other persons, and have the capacity to injure other
15 persons.

16 183. In the course of conducting their business, Defendant committed “unfair or
17 deceptive acts or practices” by, *inter alia*, knowingly failing to design, adopt, implement,
18 control, direct, oversee, manage, monitor and audit appropriate data security processes,
19 controls, policies, procedures, protocols, and software and hardware systems to safeguard and
20 protect Plaintiffs and Class Members’ Private Information, and violating the common law
21 alleged herein in the process. Plaintiffs and Class Members reserve the right to allege other
22 violations of law by Defendant constituting other unlawful business acts or practices.
23 Defendant’s above-described wrongful actions, inaction, omissions, and want of ordinary care
24 are ongoing and continue to this date.

25 184. The gravity of Defendant’s wrongful conduct outweighs any alleged benefits
26 attributable to such conduct. There were reasonably available alternatives to further
27

1 Defendant's legitimate business interests other than engaging in the above-described wrongful
 2 conduct.

3 185. As a direct and proximate result of Defendant's above-described wrongful
 4 actions, inaction, omissions, and want of ordinary care that directly and proximately caused the
 5 Data Breach and its violations of the CPA, Plaintiffs and Class Members have suffered, and will
 6 continue to suffer, economic damages and other injury and actual harm in the form of, *inter*
 7 *alia*, (1) an imminent, immediate and the continuing increased risk of identity theft, identity
 8 fraud and medical fraud—risks justifying expenditures for protective and remedial services for
 9 which they are entitled to compensation; (2) invasion of privacy; (3) breach of the
 10 confidentiality their Private Information; (5) deprivation of the value of their Private
 11 Information, for which there is a well-established national and international market; and/or (v)
 12 the financial and temporal cost of monitoring credit, monitoring financial accounts, and
 13 mitigating damages.

14 186. Unless restrained and enjoined, Defendant will continue to engage in the above-
 15 described wrongful conduct and more data breaches will occur. Plaintiffs, therefore, on behalf
 16 of themselves, Class Members, and the general public, also seeks restitution and an injunction
 17 prohibiting Defendant from continuing such wrongful conduct, and requiring Defendant to
 18 modify their corporate culture and design, adopt, implement, control, direct, oversee, manage,
 19 monitor and audit appropriate data security processes, controls, policies, procedures protocols,
 20 and software and hardware systems to safeguard and protect the Private Information
 21 entrusted to it.

22 187. Plaintiffs, on behalf of themselves and the Class Members also seek to recover
 23 actual damages sustained by each class member together with the costs of the suit, including
 24 reasonable attorney fees. In addition, the Plaintiffs, on behalf of themselves and the Class
 25 Members request that this Court use its discretion, pursuant to RCW 19.86.090, to increase the
 26 damages award for each Class Member by three times the actual damages sustained not to
 27 exceed \$25,000.00 per class member.

XI. SIXTH CLAIM FOR RELIEF

Unjust Enrichment (On Behalf of Plaintiffs, the Nationwide Class, and the Statewide Subclass)

188. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 141.

189. Defendant benefited from receiving Plaintiffs' and Members of the Classes' Private Information by its ability to retain and use that information for its own benefit. Defendant understood this benefit.

190. Defendant also understood and appreciated that Plaintiffs' and Members of the Classes' Private Information was private and confidential, and its value depended upon Defendant maintaining the privacy and confidentiality of that Private Information.

191. Plaintiffs' and Members of the Classes who were customers of Defendant's customer conferred a monetary benefit upon Defendant in the form of monies paid for services available from Defendant.

192. Defendant appreciated or had knowledge of the benefits conferred upon them by Plaintiff and members of the Classes. Defendant also benefited from the receipt of Plaintiffs' and Members of the Classes' Private Information, as Defendant used it to facilitate the transfer of Private Information between parties.

193. The monies that Plaintiffs' and Members of the Classes paid to Defendant for services were to be used by Defendant, in part, to pay for the administrative costs of reasonable data privacy and security practices and procedures.

194. Defendant also understood and appreciated that Plaintiffs' and Members of the Classes' Private Information was private and confidential, and its value depended upon Defendant maintaining the privacy and confidentiality of that Private Information.

195. But for Defendant's willingness and commitment to maintain privacy and confidentiality, that Private Information would not have been transferred to and entrusted with Defendant. Indeed, if Defendant had informed Plaintiffs' and Members of the Classes that their

1 data and cyber security measures were inadequate, Defendant would not have been permitted
2 to continue to operate in that fashion by regulators, its shareholders, and its consumers.

3 196. As a result of Defendant's wrongful conduct, Defendant was unjustly enriched at
4 the expense of, and to the detriment of, Plaintiffs' and Members of the Classes. Defendant
5 continues to benefit and profit from their retention and use of the Private Information while its
6 value to Plaintiffs' and Members of the Classes has been diminished.

7 197. Defendant's unjust enrichment is traceable to, and resulted directly and
8 proximately from, the conduct alleged in this Complaint, including compiling, using, and
9 retaining Plaintiffs' and Members of the Classes' Private Information, while at the same time
10 failing to maintain that information secured from intrusion and theft by hackers and identity
11 thieves.

12 198. As a result of Defendant's conduct, Plaintiffs' and Members of the Classes
13 suffered actual damages in an amount equal to the difference in value between the amount
14 Plaintiffs' and Members of the Classes paid for their purchases with reasonable data privacy
15 and security practices and procedures and the purchases they actually received with
16 unreasonable data privacy and security practices and procedures.

17 199. Under principals of equity and good conscience, Defendant should not be
18 permitted to retain the money belonging to Plaintiffs' and Members of the Classes because
19 Defendant failed to implement (or adequately implement) the data privacy and security
20 practices and procedures that Plaintiffs' and Members of the Classes paid for and that were
21 otherwise mandated by federal, state, and local laws and industry standards.

22 200. Defendant should be compelled to disgorge into a common fund for the benefit
23 of Plaintiffs' and Members of the Classes all unlawful or inequitable proceeds they received as a
24 result of the conduct alleged herein.

25

26

27

XII. SEVENTH CLAIM FOR RELIEF

Violation of the California Consumer Privacy Act,

(“CCPA”) Cal. Civ. Code §§ 1798.100, *et seq.* (§ 1798.150(a))

(On Behalf of Plaintiffs and the Statewide Subclass)

201. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 141.

202. Defendant had a duty to implement and maintain reasonable security procedures and practices with regard to Plaintiffs and Statewide Subclass Members' PII.

203. Plaintiffs and the Statewide Subclass Members provided to Defendant their nonencrypted and nonredacted personal information as defined in §1798.81.5 in the form of their PII.

204. Defendant violated the California Consumer Privacy Act, or CCPA, by failing to prevent Plaintiffs and Statewide Subclass Members' PII from unauthorized access and exfiltration, theft, or disclosure as a result of Defendant's violations of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the PII of Plaintiffs and Statewide Class Members.

205. As a direct and proximate result of Defendant's acts, including but not limited to its failure to encrypt its systems and otherwise implement and maintain reasonable security procedures and practices, Plaintiffs' and the Statewide Subclass Members' PII was subjected to unauthorized access and exfiltration, theft, or disclosure as a result of Defendant's violation of the duty.

206. As a direct and proximate result of Defendant's acts, including but not limited to its failure to encrypt its systems and otherwise implement and maintain reasonable security procedures and practices, Plaintiffs and the Statewide Subclass Members were injured and lost money or property, including but not limited the loss of Plaintiffs' and Statewide Class Members' legally protected interest in the confidentiality and privacy of their PII, nominal damages, statutory damages, and additional losses as described above.

207. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard Plaintiffs' and Statewide Subclass Members' PII and that the risk of a data breach or theft was highly likely. Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the PII of Plaintiff and the Statewide Class Members.

208. Defendant is a corporation organized for the profit or financial benefit of its owners, with annual gross revenues exceeding \$25 million, and collects PII as defined in Cal. Civ. Code § 1798.140.

209. Plaintiffs and the Statewide Subclass Members seek injunctive or other equitable relief to ensure Defendant hereinafter adequately safeguards Plaintiffs and the Statewide Subclass Members' PII by implementing reasonable security procedures and practices. Such relief is particularly important because Defendant continues to hold Plaintiffs and the Statewide Subclass Members' PII. These individuals have an interest in ensuring that their PII is reasonably protected.

210. Plaintiffs' counsel will send a notice letter to Defendant's registered service agents via certified mail on August 20, 2021. Assuming Defendant does not cure the Data Breach within 30 days, and Plaintiffs believe any such cure is not possible under these facts and circumstances, Plaintiffs intend to promptly amend this Complaint to seek actual damages and statutory damages of no less than \$100 and up to \$750 per customer record subject to the Data Breach on behalf of the California Class as authorized by the CCPA.

XIII. EIGHTH CLAIM FOR RELIEF

Violation of the California Unfair Competition Law, Cal. Bus. & Prof. Code § 17200, et seq. —

Unlawful Business Practices (On Behalf of Plaintiffs and the Statewide Subclass)

211. Plaintiffs and the Statewide Subclass restate and reallege the foregoing
Paragraphs 1 through 141 as if fully set forth herein.

1 212. Defendant has violated Cal. Bus. and Prof. Code § 17200, *et seq.*, by engaging in
 2 unlawful, unfair or fraudulent business acts and practices and unfair, deceptive, untrue or
 3 misleading advertising that constitute acts of “unfair competition” as defined in Cal. Bus. Prof.
 4 Code § 17200 with respect to the services provided to the California Class.

5 213. Defendant engaged in unlawful acts and practices with respect to the services by
 6 establishing the sub-standard security practices and procedures described herein; by soliciting
 7 and collecting Plaintiffs’ and Statewide Subclass Members’ PII with knowledge that the
 8 information would not be adequately protected; and by storing Plaintiffs’ and Statewide
 9 Subclass Members’ PII in an unsecure environment in violation of California’s data breach
 10 statute, Cal. Civ. Code § 1798.81.5, which requires Defendant to take reasonable methods of
 11 safeguarding the PII of Plaintiffs and the Statewide Subclass Members.

12 214. In addition, Defendant engaged in unlawful acts and practices by failing to
 13 disclose the Data Breach to California Subclass Members in a timely and accurate manner,
 14 contrary to the duties imposed by Cal. Civ. Code § 1798.82.

15 215. As a direct and proximate result of Defendant’s unlawful practices and acts,
 16 Plaintiffs and the Statewide Subclass Members were injured and lost money or property,
 17 including but not limited to the price received by Defendant for the services, the loss of
 18 Statewide Subclass Members’ legally protected interest in the confidentiality and privacy of
 19 their PII, nominal damages, and additional losses as described above.

20 216. Defendant knew or should have known that Defendant’s computer systems and
 21 data security practices were inadequate to safeguard Statewide Subclass Members’ PII and that
 22 the risk of a data breach or theft was highly likely, especially given Defendant’s inability to
 23 adhere to basic encryption standards and data disposal methodologies. Defendant’s actions in
 24 engaging in the above-named unlawful practices and acts were negligent, knowing and willful,
 25 and/or wanton and reckless with respect to the rights of members of the Statewide Subclass.

26 217. Statewide Subclass Members seek relief under Cal. Bus. & Prof. Code § 17200, *et*
 27 *seq.*, including, but not limited to, restitution to Plaintiffs and Statewide Subclass Members of

1 money or property that Defendant may have acquired by means of Defendant's unlawful, and
 2 unfair business practices, restitutionary disgorgement of all profits accruing to Defendant
 3 because of Defendant's unlawful and unfair business practices, declaratory relief, attorneys'
 4 fees and costs (pursuant to Cal. Code Civ. Proc. § 1021.5), and injunctive or other equitable
 5 relief.

6 **XIV. NINTH CAUSE OF ACTION**

7 **Violation of California's Unfair Competition Law, Cal. Bus. & Prof. Code § 17200, et seq. –**

8 **Unfair Business Practices (On Behalf of Plaintiffs and the Statewide Subclass)**

9 218. Plaintiffs and the Statewide Subclass restate and reallege the foregoing
 10 Paragraphs 1 through 141 as if fully set forth herein.

11 219. Defendant engaged in unfair acts and practices with respect to the services by
 12 establishing the sub-standard security practices and procedures described herein; by soliciting
 13 and collecting Plaintiffs' and Statewide Subclass Members' PII with knowledge that the
 14 information would not be adequately protected; by storing Plaintiffs' and Statewide Subclass
 15 Members' PII in an unsecure electronic environment; and by failing to properly dispose of
 16 equipment containing sensitive PII. These unfair acts and practices were immoral, unethical,
 17 oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiffs and
 18 Statewide Subclass Members. They were likely to deceive the public into believing their PII was
 19 securely stored, when it was not. The harm these practices caused to Plaintiffs and the
 20 Statewide Subclass Members outweighed their utility, if any.

21 220. Defendant engaged in unfair acts and practices with respect to the provision of
 22 services by failing to take proper action following the Data Breach to enact adequate privacy
 23 and security measures and protect Statewide Subclass Members' PII from further unauthorized
 24 disclosure, release, data breaches, and theft. These unfair acts and practices were immoral,
 25 unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiffs
 26 and Statewide Subclass Members. They were likely to deceive the public into believing their PII
 27

1 was securely stored, when it was not. The harm these practices caused to Plaintiffs and the
2 Statewide Subclass Members outweighed their utility, if any.

3 221. As a direct and proximate result of Defendant's acts of unfair practices, Plaintiffs
4 and the Statewide Subclass Members were injured and lost money or property, including but
5 not limited to the price received by Defendant for the services, the loss of Statewide Subclass
6 Members' legally protected interest in the confidentiality and privacy of their PII, nominal
7 damages, and additional losses as described above.

8 222. Defendant knew or should have known that Defendant's computer systems and
9 data security practices were inadequate to safeguard Statewide Subclass Members' PII and that
10 the risk of a data breach or theft was highly likely, including Defendant failure to properly
11 encrypt and dispose of equipment containing sensitive PII. Defendant's actions in engaging in
12 the above-named unlawful practices and acts were negligent, knowing and willful, and/or
13 wanton and reckless with respect to the rights of members of the Statewide Subclass.

14 223. Statewide Subclass Members seek relief under Cal. Bus. & Prof. Code § 17200, *et*
15 *seq.*, including, but not limited to, restitution to Plaintiffs and Statewide Subclass Members of
16 money or property that Defendant may have acquired by means of Defendant's unfair business
17 practices, restitutionary disgorgement of all profits accruing to Defendant because of
18 Defendant's unfair business practices, declaratory relief, attorneys' fees and costs (pursuant to
19 Cal. Code Civ. Proc. § 1021.5), and injunctive or other equitable relief.

20 **XV. PRAYER FOR RELIEF**

21 WHEREFORE, Plaintiffs, on behalf of themselves and all Class Members, requests
22 judgment against the Defendant and that the Court grant the following:

23 A. For an Order certifying the Nationwide Classes or, in the alternative, the Subclass
24 as defined herein, and appointing Plaintiffs and their Counsel to represent the certified Classes;

25 B. For equitable relief enjoining Defendant from engaging in the wrongful conduct
26 complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and the Class
27

- 1 Members' PII, and from refusing to issue prompt, complete, any accurate disclosures to the
- 2 Plaintiffs and Class members;

3 C. For injunctive relief requested by Plaintiffs, including but not limited to,
4 injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and
5 Class Members, including but not limited to an order:

1. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;
2. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;
3. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiffs and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members ;
4. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the personal identifying information of Plaintiffs and Class Members' personal identifying information;
5. prohibiting Defendant from maintaining Plaintiffs' and Class Members' personal identifying information on a cloud-based database;
6. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering

Defendant to promptly correct any problems or issues detected by such third-party security auditors;

7. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;
8. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;
9. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant’s network is compromised, hackers cannot gain access to other portions of Defendant’s systems;
10. requiring Defendant to conduct regular database scanning and securing checks;
11. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees’ respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiffs and class members;
12. requiring Defendant to conduct internal training and education routinely and continually, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;
13. requiring Defendant to implement a system of tests to assess its respective employees’ knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees’ compliance with Defendant’s policies, programs, and systems for protecting personal identifying information;

14. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;
15. requiring Defendant to meaningfully educate all class members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;
16. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and
17. for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment; and

For an award of damages, including actual, nominal, and consequential damages, law in an amount to be determined;

For an award of punitive damages;

For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

For prejudgment interest on all amounts awarded; and

Such other and further relief as this Court may deem just and proper.

XVI. DEMAND FOR JURY TRIAL

Plaintiffs hereby demand that this matter be tried before a jury.

1 RESPECTFULLY SUBMITTED AND DATED this 19th day of August, 2021.

2 TERRELL MARSHALL LAW GROUP PLLC

3 By: /s/ Beth E. Terrell, WSBA #26759

4 Beth E. Terrell, WSBA #26759

5 Email: bterrell@terrellmarshall.com

6 936 N. 34th Street, Suite 300

7 Seattle, Washington 98103

8 Telephone: (206) 206-816-6603

9 Facsimile: (206) 319-5450

10 M. Anderson Berry*

11 Email: aberry@justice4you.com

12 CLAYEO C. ARNOLD, A PROFESSIONAL
13 LAW CORP.

14 865 Howe Avenue

15 Sacramento, California 95825

16 Telephone: (916) 777-7777

17 Facsimile: (916) 924-1829

18 Gary E. Mason*

19 Email: gmason@masonllp.com

20 David K. Lietz*

21 Email: dlietz@masonllp.com

22 MASON LIETZ & KLINGER LLP

23 5101 Wisconsin Avenue NW, Suite 305

24 Washington, DC 20016

25 Telephone: (202) 429-2290

26 Facsimile: (202) 429-2294

27 Gary M. Klinger*

Email: gklinger@masonllp.com

MASON LIETZ & KLINGER LLP

227 W. Monroe Street, Suite 2100

Chicago, Illinois 60606

Telephone: (202) 429-2290

Facsimile: (202) 429-2294

1 William Howard*
2 Email: Billy@TheConsumerProtectionFirm.com
3 THE CONSUMER PROTECTION FIRM
4 401 East Jackson Street, Suite 2340
5 Truist Place
6 Tampa, Florida 33602
7 Telephone: (813) 500-1500
8 Facsimile: (813) 435-2369

9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
Attorneys for Plaintiffs and the Classes

**Pro hac vice forthcoming*